Overzicht van vragen en bezwaren bij de consultatie “NL GOV OpenID Connect profiel (standaard voor veiliger internet)”

- In het toepassingsgebied lijkt geen rekening gehouden te worden met authenticatie routatie , token translatie en machtigingen. Waarom is dit niet geen onderdeel van het toepassingsgebied aangezien dit essentiële onderdelen zijn van bijvoorbeeld eHerkenning en DigiD?

- Waarom is er gekozen om een profiel te ontwikkelen voor de Nederlandse overheid, en niet een internationaal erkend profiel gehanteerd?

- Welke profielen zijn overwogen als standaard voor OpenID connect en waarom is besloten deze niet te hanteren of deze niet aan te passen?

- In het expertadvies wordt meerdere malen gewezen op het probleem dat er andere OIDC profielen zijn welke al gebruikt worden door de overheid. Waarom wordt niet een van deze profielen in overweging genomen als standaard voor de Nederlandse overheid? Hoe vergelijken deze profielen zich met het NL GOV profiel?

- Welke aanleiding heeft de overheid om aan te nemen dat deze nieuwe standaard ondersteund kan worden door (inter)nationale software ontwikkelaars? Hoe kan de Nederlandse overheid aantonen dat dit protocol geen oneigenlijke concurrentie veroorzaakt tussen Nederlandse en Europese aanbieders van software?

- Is er onderzoek gedaan of er softwarepakketten op de markt zijn die dit profiel kunnen hanteren? Indien dit het geval is, welke softwarepakketten zijn hiervoor gebruikt?

- Is de overheid bereid om de kosten te betalen voor het aanpassen van als bestaande software, bijvoorbeeld het migreren van bestaande OIDC koppelingen naar het NL GOV OpenID Connect profiel?

- Waarom voldoet dit profiel niet aan de criteria voor toetsing van een standaard? Wat is er uit de initiële analyse gekomen en zijn er meer onderdelen die niet conform de criteria zijn maar niet genoemd worden in dit document?

- Moet er nog een aanpassing komen op het NL GOV OpenID Connect profiel om in aanmerking te komen om een standaard te worden?

- Welke partijen hebben opgeroepen om een nieuw OIDC profiel te maken (dus niet de partijen die meegewerkt hebben om het profiel uit te werken), aangezien er al verschillende authenticatieprotocollen staan op de “pas toe of leg uit” lijst staan die dezelfde functionaliteit bieden?

- Wat is onderscheidend aan het NL GOV OpenID Connect profiel ten opzichte van andere OICD profielen, Oauth, SAML of andere protocollen op de “pas toe of leg uit” lijst?

- Op wat voor een manier gaat het NL GOV OpenID Connect profiel Nederland veiliger maken dan de andere authenticatie protocollen welke al aanwezig zijn op de “pas toe of leg uit” lijst?

- In het NL GOV OpenID Connect profiel is geen voorziening voor de encryptie van attributen, wat bijvoorbeeld wel nodig is voor eHerkenning. Er is alleen een voorziening voor de encryptie het gehele bericht. Hierdoor is het profiel niet meer geschikt om in te zetten bij de generieke routeringsvoorziening of de eHerkenning makelaar aangezien zij anders alle inhoudelijke berichten

kunnen meelezen en de beveiliging dus verminderd wordt. Zijn er plannen om deze functionaliteit als nog in het NL GOV OpenID Connect profiel te plaatsen?

- Op dit moment is er nog geen functionele beschrijving van de verschillen tussen SAML, OpenID connect, Oauth en andere federatieve authenticatie protocollen op de “pas toe of leg uit” lijst. Komt er nog een uitleg wat het onderscheidend vermogen van deze profielen afzonderlijk zijn en wanneer een bepaald profiel gekozen moet worden?

- De uitwerking van het NL GOV OpenID Connect profiel is onvoldoende getest / bewezen practisch haalbaar te zijn om de Nederlandse overheid te vereisen dit onderdeel te maken van huidige of toekomstige implementaties. Waarom is er dan toch voor gekozen om het NL GOV OpenID Connect profiel op een lijst met af te dwingen protocollen te plaatsen?

- Waar moet het NL GOV OpenID Connect profiel komen op de "‘pas toe of leg uit’-lijst"? Is dit bij de categorie verplichte standaarden of aanbevolen standaarden?

- De doelstelling zoals genoemd in Hoofdstuk 3 komt niet overeen met het werkingsgebied uit hoofdstuk 4. Mist het NL GOV OpenID Connect profiel daarmee niet het gewenste doel?

- Dit expertadvies geeft geen uitleg over de volgende gestelde doelen van het NL GOV OpenID Connect profiel:

1. Het neerzetten van een fatsoenlijke baseline voor privacy en security.
2. Maar de standaard moet ook toepasbaar zijn voor bi- en multilaterale afspraken tussen partijen,
3. zelfs intern een organisatie.
4. Het moet ook schaalbaar zijn

Kan hierbij gesteld worden dat de doelen van het NL GOV OpenID Connect profiel niet gehaald zijn, of dat de uitwerking om deze doelen te halen nog plaats moet vinden?

- Wat is het verschil in het toepassingsgebied van OIDC ten opzicht van het verwerkingsprofiel van het NL GOV OpenID Connect profiel? Welke van deze 2 verschillende toepassingsgebieden zal gebruikt worden voor het NL GOV OpenID Connect profiel?

- In het verwerkingsgebied worden organisaties genoemd die namens de overheid authenticatievoorzieningen bieden. Zij vallen daarmee binnen het verwerkingsgebied, betekent dit dan ook dat zij intern het NL GOV OpenID Connect profiel moeten hanteren, of alleen het NL GOV OpenID Connect profiel moeten hanteren voor de diensten die deze partij aan de overheid bied?

- In paragraaf 5.1.1.3 van het expertadvies word positief geantwoord op de vraag of het NL GOV OpenID Connect profiel generiek toepasbaar is. Dit is niet correct aangezien dit profiel:

A: Alleen voor de Nederlandse overheid en zijn uitvoerders is volgens het werkingsgebied

B: Er geen softwareaanbieders zijn die dit profiel kunnen bieden op dit moment.

C: OIDC een generieke standaard is, maar door de wijzigingen die het NL GOV OpenID Connect profiel toepast is het OIDC protocol niet meer generiek is (het is immers specifiek gemaakt voor de Nederlandse overheid).

Hoe kunnen de experts daarom aantonen dat het NL GOV OpenID Connect profiel bruikbaar is buiten het werkingsgebied en daarmee generiek toepasbaar is?

- In paragraaf 5.1.2.1 van het expertadvies word eerst beargumenteerd dat SAML naast OpenID Connect kan worden gehanteerd. Enkele regels later wordt gesuggereerd SAML toch van de lijst af te halen? Waarom moet SAML van de lijst afgehaald worden, voldoet deze niet meer aan de eisen die eraan gesteld worden / is het aannemelijk te maken dat deze standaard niet meer voldoet aan de gestelde eisen? Op dit moment lijkt het er namelijk op dat SAML moet worden weggehaald om ruimte te bieden voor het NL GOV OpenID Connect profiel omdat er anders geen business case is.

- In paragraaf 5.1.2.2 van het expertadvies wordt gesteld dat OIDC meer toepasbaar is dan SAML in mobiele scenario's, dit is alleen niet in scope van het toepassingsgebied. Waarom wordt dit dan als onderscheidend vermogen aangemerkt aangezien dit niet onderdeel is van het toepassingsgebied?

Daarnaast is er een protocol op de lijst die mobiele authenticatie wel specifiek de mobiele authenticatie in scope heeft (oAuth). Waarom wordt er wel een vergelijk gemaakt met SAML maar niet oAuth en het profiel dat daarvoor ontwikkeld is?

- In paragraaf 5.1.2.2 van het expertadvies wordt gesteld dat SAML niet meer doorontwikkeld kan worden. Dit is incorrect aangezien de ontwikkelmogelijkheden van de SAML standaard zijn bewezen door de overheid in de uitvoerige wijzigingen die eTD aan dit protocol heeft gemaakt. In de laaste jaren is gebleken dat er nog steeds mogelijkheden zijn om het protocol aan te passen.

- In paragraaf 5.1.2.2 van het expertadvies wordt gesteld dat "De adoptie en doorontwikkeling van de OpenID Connect standaard is groter dan bij SAML" Waar blijkt dit uit, is dit aan te tonen?

- In paragraaf 5.1.2.2 van het expertadvies wordt gesteld dat "Daarnaast spitst het NL GOV OpenID Connect profiel specifiek zich toe op de context van (semi-)overheidsorganisaties in Nederland." spreekt dit niet de generieke aard tegen zoals beargumenteerd in paragraaf 5.1.1.3? Indien dit niet het geval is hoe kan deze specifieke toelegging dan alsnog generiek ingezet worden?

- In paragraaf 5.1.2.3 van het expertadvies wordt gesuggereerd dat oAuth geen mogelijkheid heeft om authenticatie- en identiteitsgegevens uit te wisselen. Dit is niet correct Oauth bied naast autorisatie ook de mogelijkheid van authenticatie en gegevensuitwisseling, waarom is dit niet meegenomen in het NL GOV OAuth 2.0 profiel?

- Het NL GOV OAuth 2.0 profiel is geen onderdeel van de OAuth2 standaard op de "pas toe of leg uit-lijst". Waarom is dit niet nodig voor OAuth, maar moet wel een profiel worden verplicht voor Openid connect?

- In paragraaf 5.1.2.4 van het expertadvies wordt onterecht gesuggereerd dat het Nederlandse profiel beheerd wordt door de OpenID connect Foundation. Dit profiel is geen onderdeel van OpenId connect en kan daarmee ook niet beheerd worden door de OpenID connect Foundation.

- In paragraaf 5.1.3.1 van het expertadvies wordt gesteld dat de kosten acceptabel zijn. Heeft de expertgroep de kosten voor implementatie berekend, en wat zijn deze kosten dan? Daarnaast is het niet duidelijk volgens welke criteria dit bestempeld zijn als acceptabele kosten. Hoe is de expertgroep tot deze conclusie gekomen?

- De kosten voor de implementatie van het NL GOV OpenID Connect profiel zullen volgens het verwerkingsgebied alleen gemaakt worden voor de overheid en de dienstverleners die namens de overheid werken. Hierdoor is het NL GOV OpenID Connect profiel niet generiek inzetbaar en dus relatief duur TOV het bereik van een internationaal profiel of het bereik van een generiek profiel voor alle nationale doeleinden. Is deze overweging ook meegenomen in de berekening van de acceptabele kosten?

- Aangezien het NL GOV OpenID Connect profiel nog niet uit ontwikkeld is, zijn de uiteindelijke kosten daarom nog niet bekend. Dit profiel kan dus nog vele malen duurder worden. Hoe kan de expertgroep daarom bepalen dat de implementatiekosten acceptabel zijn?

- het NL GOV OpenID Connect profiel wordt het volgende advies gegeven: "De expertgroep geeft aan de beheerders het advies om conformerende configuraties van gangbare implementaties van het profiel beschikbaar te stellen" Dit is met klem af te raden omdat dit kan leiden tot een beveiligingsbreuk van de desbetreffende webapplicaties. Als security configuratie publiek wordt kan een kwaadwillende gebruiker hier immers misbruik van maken. Kan de expertgroep toelichten hoe deze vorm van misbruik voorkomen kan worden?

- Waarom is het goedkoper om een nieuw OIDC profiel te implementeren ten opzichte van een SAML dialect? Is hier een inschatting gemaakt van kosten / inzet / complexiteit door de werkgroep en kan deze inschatting inzichtelijk gemaakt worden?

- In paragraaf 5.1.3.2 van het expertadvies staat dat het NL GOV OpenID Connect profiel de security laat toenemen. Hoe is dit het geval aangezien enkele security features die wel in SAML en OAuth zitten weggelaten worden? Zijn er andere zaken toegevoegd die de security doen toenemen? Kan de expertgroep dit toelichten?

- In paragraaf 5.1.3.2 van het expertadvies staat dat het NL GOV OpenID Connect profiel de privacy laat toenemen. Zijn er zaken toegevoegd die de privacy beter waarborgen dan SAML of OAuth dat kan? Kan de expertgroep dit toelichten?

Als laatste wil ik voor deze paragraaf toelichten dat het toevoegen van het NL GOV OpenID Connect profiel niet een belangrijke enabler is van het profiel, maar de enige. Zonder toevoeging op deze lijst is er geen indicatie dat er andere partijen of overheden zijn die dit profiel gaan implementeren. Daarmee lijkt er dus geen duidelijke businesscase te zijn voor dit profiel. Waarom is dit niet benadrukt in deze paragraaf?

- In paragraaf 5.1.3.23 van het expertadvies wordt op de volgende zaken geen toelichting gegeven:

* Waarom is de meerwaarde van het NL GOV OpenID Connect profiel niet inzichtelijk te maken? Indien deze er niet is, is er dan wel een businesscase voor dit profiel?

* Waarom is het niet mogelijk de impact op de bedrijfsprocessen inzichtelijk te maken aangezien het implementeren van de standaard betekent dat de overheid meer kosten moet maken om authenticatie en authorisatie in een federatieve omgeving te implementeren. Dit suggereert dus dat er geen meerwaarde is aan het protocol, maar wel meer kosten!

De daadwerkelijke meerwaarde van dit profiel is niet genoemd ten opzichte SAML en OAuth binnen de gestelde scope. Is het niet aannemelijk te maken dat er meerwaarde is, en zo nee, wat is dan de meerwaarde binnen de scope van het toepassingsgebied?

- In paragraaf 5.1.3.4 van het expertadvies word gesteld dat het profiel de beveiliging van het OIDC protocol verbeterd. Op wat voor wijze verbetert het profiel de beveiling van OICD protocol en brengt het de genoemde veiligheid?

- In paragraaf 5.1.3.5 van het expertadvies word gesteld dat het profiel de privacy verhoogd door dataminimalisatie bij uitvraag van attributen. Dit is een drogreden omdat dataminimalisatie geen onderdeel is van het profiel zelf, maar van het beleid dat de overheid voert. Het profiel kan namelijk de overheid niet controleren of er te veel informatie wordt uitgevraagd. Hierdoor is de privacy niet

gewaarborgd door het profiel, maar door het beleid van de overheid, hetwelk geen onderdeel is van dit advies.

- In paragraaf 5.1.4 van het expertadvies word geconcludeerd dat het profiel een grote toegevoegde waarde heeft door de eenduidigheid van de implementaties. De beargumenteerde toegevoegde waarde bestaat niet aangezien OICD al meerdere profielen kent, net zoals SAML meerdere dialecten kent. Omdat er geen internationale standaard gekozen is kan zelf geargumenteerd worden dat dit profiel in de toekomst voor meer problemen gaat zorgen aangezien dit profiel internationaal niet bruikbaar is. Hoe is de expertgroep dan toch tot de conclusie gekomen dat dit een grote toegevoegde waarde heeft?

In paragraaf 5.2.1.2 van het expertadvies word gesteld dat het beheersproces is ingeregeld en toegankelijk is; hoe kan dit beschikbaar zijn als het beheerproces nog niet voldoende is ingeregeld volgens hoofdstuk 1?

In de voorgaande paragraaf wordt gesteld dat de notulen beschikbaar zijn;  de notulen van de werkgroep zijn beschikbaar tot 14-5-2020 en daarmee niet volledig. Daarnaast zijn de notulen vanaf het begin tot en met 9 jan zijn de documenten verkeerd opgeslagen waardoor ze niet meer te lezen zijn (folders met metadata IPV office documenten).

In paragraaf 5.2.3.3 van het expertadvies word gesteld dat er formeel bezwaar kan worden aangetekend omdat de Gitlab omgeving open is voor het publiek. Het aanmaken van een issue in Gitlab is iets anders als een formeel bewaar aantekenen. Om een formeel bezwaar aan te tekenen moet degene die dat wil doen bijvoorbeeld het volgende kunnen:

1: Een overheidsorgaan moet aan te schrijven zijn om het bezwaar in te dienen. Deze informatie is niet beschikbaar op gitlab

2: Via gitlab kan een bezwaar niet ondertekend met DigID, wat wel een vereiste is voor een formeel bezwaar.

3: Deze gitlab is niet opgenomen in het register van overheidsinstanties waar bewaar kan worden ingediend.

Hierdoor kan er dus geen formeel bezwaar worden aangetekend voordat het profiel op de lijst komt en dit beschikbaar wordt gemaakt door het forum standaardisatie.

In paragraaf 5.2.6.2  van het expertadvies word gesteld dat er geen daadwerkelijke ondersteuning die geboden wordt door de overheid als het aankomt op geschillen van inzicht bij de implementatie bijvoorbeeld. Hoe kan er dan voor gezorgd worden dat de standaard correct wordt geïmplementeerd? Hoe kan het forum standaardisatie dan ook andere vragen beantwoorden en deze standaard uitdragen?

In paragraaf 5.3 van het expertadvies word gesteld dat aanbieders en gebruikers voldoende positieve ervaring hebben met het protocol OIDC. Ik vind het verontrustend dat het NL GOV OpenID Connect profiel gelijk wordt getrokken met het onderliggende protocol. Het protocol is daadwerkelijk iets anders dan het profiel.

Daarnaast hebben gebruikers ervaring gebaseerd op andere OICD profielen. Er is geen indicatie dat het NL GOV OpenID Connect profiel dezelfde ervaring oplevert als andere profielen. Hoe kan de expertgroep dan concluderen dat er positieve ervaringen zijn met dit profiel?

Daarnaast is het verontrustend dat tijdens een hackaton (waarin deelnemers exclusief bezig zijn met de implementatie van het protocol) de deelnemers het niet voor elkaar krijgen om het volledige NL GOV OpenID Connect profiel te implementeren. Dit impliceert dat het protocol slecht implementeerbaar is en dus voor meer kosten gaat zorgen. Hoe kan de expertgroep dan stellen dat de aanbieders, zonder het NL GOV OpenID Connect profiel volledig werkend te krijgen, positieve ervaringen hebben met het NL GOV OpenID Connect profiel? Is dit niet een duidelijke indicatie van het tegenovergestelde en een indicatie om een andere weg in te slaan?

Ik zie graag het antwoord tegemoet op de bovenstaande vragen en wil de expertgroep oproepen om de genoemde bewaren in overweging te nemen.

Met collegiale groet

Dhr. Ing. A.Z.N van Pelt